

**SEALED**FILED IN UNITED STATES DISTRICT  
COURT, DISTRICT OF UTAHAUG 07 2019  
BY D. MARK JONES, CLERK  
DEPUTY CLERK

## UNITED STATES DISTRICT COURT

for the  
District of UtahIn the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

See Attachment A-1

Case No. 2:19-mj-558-DBP

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):  
See Attachment A-1

located in the \_\_\_\_\_ District of \_\_\_\_\_ Utah \_\_\_\_\_, there is now concealed (identify the person or describe the property to be seized):  
Items listed in Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 USC 1349, 1344, 1028A, 1956	Conspiracy to Commit Bank Fraud, Bank Fraud, Aggravated Identity Theft, Money Laundering

The application is based on these facts:  
See attached affidavit incorporated herein by reference

- ☒ Continued on the attached sheet.  
☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

TFO Justin Hansen

Printed name and title

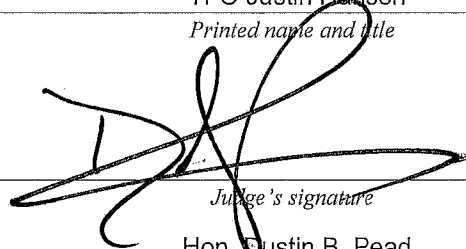
Sworn to before me and signed in my presence.

Date:

8/7/19

City and state:

SLC, UT



Judge's signature

Hon. Justin B. Pead

Printed name and title

**AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT**

I, Justin Hansen, being first duly sworn, hereby depose and state as follows:

**I. PURPOSE**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search and seize evidence, fruit, and/or instrumentalities of certain offenses as described in Attachment B, at the following locations, vehicles, and persons, in the District of Utah, as more fully described in Attachments A-1 through A-3:

- a. The residence located at 3355 South Riviera Drive, South Salt Lake City, Utah, as further described in Attachment A-1;
- b. The Black 2007 Cadillac Escalade with Utah License Plate 5F9HU and VIN 3GYFK62837G226611, as further described in Attachment A-2; and
- c. The person TALALIMA TOILOLO (age 44), as further described in Attachment A-3.

**II. INTRODUCTION AND AGENT BACKGROUND**

2. I am an Agent with the State Bureau of Investigations for the State of Utah, I have been an investigative or law enforcement officer for the State of Utah since October of 2001. I have been trained or investigated cases involving homicides, suicides, theft, false documentation, violent crimes, illegal drug operations, child exploitation, and sexual assaults. Your affiant's specialized training includes training on drug trafficking and interdiction, gang suppression and enforcement and violent crime investigations. Your affiant is currently a task force officer with the Salt Lake City, FBI, Violent Crime Task Force.

3. The facts in this affidavit are based on my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. FBI and the California Regional Enforcement Allied Computer Team (REACT)

Task Force conducted much of the investigation described below. REACT is a partnership of California local, state, and federal agencies formed in cooperation with private industry to investigate technological crime. REACT conducts multi-jurisdictional investigations including stolen high technology, identity theft, and other computer related crimes.

5. Based on the facts set forth in this affidavit, there is probable cause to believe that Jonathon WARD, Talalima TOILOLO (aka “Lima” and “Nua”), and Monica NUNES committed acts in violation of 18 U.S.C. §§ 1349 (conspiracy to commit bank fraud), 1344 (bank fraud), 1028A (aggravated identity theft), and 1956 (money laundering). There is also probable cause to search the information described in Attachment A for evidence of these crimes and further described in Attachment B.

### **III. PROBABLE CAUSE**

#### **The Criminal Acts**

6. This investigation has shown that WARD, NUNES, TOILOLO, and others yet to be named, acquired “Point of Sale” (POS) terminals by either purchase or theft and manipulated them to make fraudulent merchant refunds starting in or about June 2018, and continuing until in or about February 2019. Based on my discussions with the investigators in this case, it is believed TOILOLO continued this fraud scheme to the present with other co-conspirators after WARD and NUNES arrests in February 2019. This investigated bank fraud scheme is referred to as “Forced Post Refund Fraud” or “Refund Fraud”. The scheme exploits the refund process of the merchant accounts of various banks and payment processors. A merchant account is a type of bank account that allows businesses to accept payments via multiple electronic methods, typically using debit and credit cards (“access cards”). Such an account is established under an agreement between a merchant (e.g., a retail establishment) and a merchant acquiring bank for the settlement of access card transactions. The acquiring bank processes credit or debit card payments on behalf of the merchant.

7. When a legitimate business wants to accept access cards as payment for merchandise or services, they open a merchant account with an acquiring bank to manage funds

and process credit and debit transactions. For example, when a merchant makes a sale and accepts payment via an access card, they enter the amount of the sale and then “swipe” the access card on a POS terminal. The terminal reads the magnetic stripe on the rear of the access card and processes the purchase by electronically transmitting a request to initiate a transfer of funds from the access card holder’s account to the merchant’s account. This transaction is completed by a bank directly or via a payment processor over phone lines or the internet.

8. Although some acquiring banks act as their own processor to process payment and refund transactions involving access cards, others employ a specific payment processing company (“payment processor”) to process the payments and refunds for them. A payment processor can be appointed by a merchant to handle transactions from various channels such as credit and debit cards for the merchant acquiring banks.

9. In general, when a payment processor is used to process card transactions, the merchant’s POS terminal transmits a merchant ID number and other information to the payment processor indicating that the transaction is legitimate. In an operation that will usually take a few seconds, the payment processor will check the transmission data by forwarding it to the respective access card’s issuing bank or card association (e.g., Visa) for verification. Once the payment processor has received confirmation that the credit card details are verified, the information will be relayed back via a payment gateway to the merchant, who will then complete the payment transaction. The funds are then transferred from the purchaser’s/access card user’s account and deposited into the merchant’s account.

10. Similarly, when a merchant requests a refund of a purchase they again swipe the purchaser’s access card at the POS terminal and enter the refund amount. The POS terminal reads the magnetic strip on the rear of the access card and processes the refund. The refund amount is then deducted from the merchant’s account and credited to the access card’s account.

11. The refund fraud scheme also requires a POS terminal to communicate with a payment processing company or service (via phone lines or the Internet) situated between the merchant and the merchant bank. The perpetrators then fraudulently set-up the terminals using

phone lines, the internet, or other electronic devices, so that payment processors and banks falsely recognize the terminals as being linked to a particular merchant and merchant account. They then used the terminals to process false refund transactions when no purchases were ever made. I am aware that perpetrators of this scheme will often store information such as access device numbers, PIN numbers and merchant ID numbers on electronic devices, and may use these electronic devices in the facilitation of the scheme.

12. Using one or more POS terminals that were reprogrammed with new merchant account information, WARD, TOILOLO, and NUNES executed fraudulent refunds, even though no purchases were ever made. During this fraudulent refund process, the payment processor or bank, believing that the transmitted request for refunds came from the true merchant(s), transmitted false refund money to the access card account. WARD, TOILOLO, and NUNES then depleted the access card by using it to make purchases, ATM cash withdrawals, and money order purchases. These fraudulent refunds resulted in losses to the banks holding the merchant accounts. The victim merchants likely did not realize the funds were withdrawn until they checked their bank statements, which may have taken days or even weeks. By that time, the money had been transferred from the merchant bank account to the access card accounts and often removed from the card accounts via subsequent purchase or transfer.

13. Matsuda's Nursery is a business located at 10600 Florin Road, Sacramento, California, in the Eastern District of California whose merchant payment processor is also Worldpay/Vantiv. WARD and NUNES were never employed by that business. Additionally, the hours of operation for Matsuda's are Monday through Friday, 7:00 am through 4:30 pm. Matsuda's was identified as a victim of this fraud. Matsuda's merchant account is with Wells Fargo, a bank that is FDIC insured.

14. Instant Storage is a business located at 301 State Road, Bakersfield, California, in the Eastern District of California whose merchant payment processor is also Worldpay/Vantiv. WARD and NUNES were never employed by Instant Storage. Additionally, the hours of operation for Instant Storage are Monday through Friday, 8:00 am through 5:00 pm. Instant

Storage was identified as a victim of this fraud. Instant Storage's merchant account is with Bank of America, a bank that is FDIC insured.

15. In July 2018, REACT investigators were investigating WARD, TOILOLO, and NUNES after identifying them as participants in this bank fraud scheme against at least Instant Storage as discussed herein. REACT investigators knew that the suspects often conducted refund fraud from various hotels. Based on my experience and discussions with other law enforcement personnel, criminals often conduct fraud schemes from hotels to hide their true identities and the location of incriminating evidence. On September 21, 2018, REACT investigators obtained a federal search warrant to track a mobile device having phone number 415-516-7613, which was a phone number associated with WARD. On October 12, 2018, REACT investigators tracked WARD and NUNES to a Pleasanton Marriot, located at 11950 Dublin Canyon Road, Pleasanton, California. At that time, the REACT investigators knew that both WARD and NUNES were on searchable probation, and they suspected that WARD and NUNES were involved in Refund Fraud. REACT officers then contacted WARD and NUNES in and around WARD's vehicle, a Black Cadillac Escalade, in the parking lot of the Pleasanton Marriot, and conducted a search of the Cadillac.

16. During the Cadillac search, officers found a loaded handgun and a personal use amount of methamphetamine. Both WARD and NUNES were convicted felons, and officers arrested them that day on gun and drug charges. REACT officers also located and seized multiple access cards and WARD's and NUNES' cellular phones from the Cadillac. Additionally, WARD had the following items in his wallet at the time of his arrest (the list is not exhaustive):

- a) A Key Bank debit card ending x2088 and having the name "Jonathon Ward"; and
- b) A PayPal card ending x8910 and embossed with the name "Jonathon Ward".

17. NUNES had the following item (among other items of evidentiary value) in her purse at the time of her arrest: a receipt dated October 12, 2018 showing the purchase of \$50.00 worth of credits from a Recharge Kiosk at Boomers (miniature golf/go karts) in Livermore

purchased with PayPal card ending x8910.

18. REACT investigators learned that WARD and NUNES had directed the relocation of specific items of evidence and contraband to 3150 Mills Drive, Brentwood, California, to avoid law enforcement detection and seizure, which was the residence of WARD's sister. Investigators then obtained a state search warrant to search that residence and executed the search on October 17, 2018. Among the items seized at the residence were:

- a) Nine POS terminals;
- b) A Wells Fargo debit card ending x7922 and having the name Monica Nunes;
- c) A handwritten note detailing a script for a conversation to Mercury Payments regarding a JW Rental account at Paypal;
- d) Nine Blank access cards, one of which had the name of "Johnathon Ward" on the magstripe;<sup>1</sup>
- e) Two cellular phones in WARD's possession.

#### **Recovered Text Messages Between WARD and TOILOLO**

19. A search warrant was obtained by the REACT Task Force to forensically access and examine the phones seized during the October 12, 2018, arrest for evidence of refund fraud. The examination included the review of text messages. Investigators confirmed one phone belonged to WARD due to phone records and photos of WARD on the phone. Investigators discovered multiple messages between WARD and TOILOLO. During the investigation, Investigators determined that at least two phone numbers (859-206-4443 and 859-307-6778) that WARD was texting were being used by TOILOLO. Investigators determined this based on at least the following information:

- a) On October 16, 2018, WARD called his sister, Nicole Ward, from jail and she initiated a three-way call with "Nua" (TOILOLO's alias). WARD asked TOILOLO to move all his stuff out of a house in Sacramento and TOILOLO gave

---

<sup>1</sup> This card was a blank, i.e., it had no markings on it and only a magstripe affixed to it. The card number and the name information were gleaned from the encoded magstripe and subsequently verified by Metropolitan Commercial Bank. Based on my training and experience, criminals use blank access cards to encode credit/debit account information for facilitating fraud schemes.



him his new number: 859-307-6778.

- b) On October 17, 2018, NUNES made a jail call to “Nua” (TOILOLO’s alias) using one of these numbers and asked him to get her account info from Nicole Ward and wipe her phone. Nua said he would take care of it.
- c) TOILOLO referred to his daughter as “Sabrina” and “Bree” in some of the text messages. TOILOLO has a daughter, Sabrina Toilolo.
- d) On August 1, 2018, TOILOLO texted WARD to send him some items relating to their scheme, and TOILOLO provided an address in UT that is the residence of his child’s mother.
- e) On September 21, 2018, TOILOLO texted WARD to send him some money via PayPal and provides the address: catrina.toilolo@gmail.com, which is the name of the mother of TOILOLO’s child.
- f) On October 2, 2018, TOILOLO texted WARD to send him some money and WARD responded, “How much to send?” TOILOLO responded, “Send as much as u can of that 5,” and the texted, “Talalima Toilolo SLC UTAH,” presumably for a money wire.

20. The text messages between TOILOLO and WARD show their knowledge of their crime and sharing knowledge of the fruits of the crime. The text message stream below was from WARD’s phone and occurred on August 1, 2018:

TOILOLO to WARD 3:37 PM – “Me too I got Vantiv to hit one time one ticket but for only 180.00 that was it”

TOILOLO to WARD 3:38 PM – “This shit stressful blood u guys got any d nobody got work out here past 2 days this shit crazy”

WARD to TOILOLO 3:39 PM – “Send address”

TOILOLO to WARD 3:40 PM – “3355 S Riviera Dr SLC UT 84106” “Yes please ain't gotta b much”

TOILOLO to WARD 7:44 PM – “Y'all still working”



WARD to TOILOLO 7:56 PM – “Yip”

It is common in this fraud scheme, it was common to view proceeds of fraud wired from one co-conspirator to another based upon their participation in the scheme.

21. Investigators further reviewed text messages between WARD and know co-conspirator Connie RAMOS on July 3, 2018:

WARD to RAMOS at 10:30 PM – “Whats up is where the 500 owed”

RAMOS to WARD at 10:34 PM – “I don’t owe you \$500” “You only put 15 on their – 400 left 1100 that’s 370 each”

Much of the communication between WARD and RAMOS includes the sharing of access card numbers later used for refund fraud, the division of money obtained through refund fraud, the direction by WARD to wire money to others involved in the conspiracy, and the sharing location information to allow RAMOS and WARD to meet to commit refund fraud.

22. The forensic examination of WARD’s two cellphones (seized in October 2018) show that TOILOLO was a member of the conspiracy and regularly texted WARD to further the scheme. Particularly, TOILOLO supplied WARD with numerous TID numbers and access card numbers beginning in June 2018 and ending no earlier than October 9, 2018. The merchants associated with these TID numbers – including, for example, Holland Home Care, Merced Honda, and Supreme Power Sports LLC – were victims of refund fraud around the time of the texts. The TID is the number programmed into a POS terminal, which allows the terminal to act as the merchant. The TID is unique to each company and required to complete the refund fraud.

23. For example, TOILOLO texted the TID number for Merced Honda and Supreme Power Sports on August 15 and these merchants suffered refund fraud on August 15–17. The text messages also show the two discussing whether the TID numbers were successful and the handling of fraud proceeds. According to Vantiv/WorldPay records, both Merced Honda and Supreme Power Sports LLC were victims in the above detailed fraud scheme. Merced Honda in Merced, California for approximately \$3,400.00 between August 15, 2018 and August 17, 2019 and Supreme Power Sports LLC Lewiston Idaho from August 16, 2018 to August 20, 2018 for

approximately \$9,500.00.

### **TOILOLO's Use of an Access Device Linked to Refund Fraud**

24. A Wells Fargo debit card x4989 registered to Victim 1 was used to make \$55,000 in false purchases from Fontano's Subs on January 22, 2019. It is likely that the conspirators used terminals to make this type of false purchases, as opposed to a refund, to pre-test whether a particular terminal and TID would work, and to provide a purchase prerequisite for the fraudulent refunds. These purchases were made just prior to fraudulent refunds being charged to the same merchant account using two different access devices linked to WARD. Surveillance video shows TOILOLO using the x4989 card at an ATM on January 21, 2019. On that same day, the same card was used to make another false purchase from merchant Take 5 Oil. That merchant was a victim of refund fraud in August 2018.

### **Evidence Obtained via Previous Federal Search Warrants**

25. On April 25, 2019, Eastern District of California Magistrate Judge Carolyn K. Delaney signed a search warrant associated with Apple, Inc accounts canuseeme57@icloud.com, only1daddy4u@icloud.com, and ognunes100@icloud.com.

26. Agents observed the following images and documents contained within accounts provided by Apple Inc in association with the search warrant:

- a) An email dated December 5, 2018 from John Ward only1daddy4u@icloud.com with message "4722... pin ..2323" "2844...pin 0211" "6874...pin 2018". Based on my experience and discussions with other law enforcement, the numbers in this case represent the last four numbers of debit card numbers and the associated pin numbers. During the execution of fraud schemes exploiting debit cards, conspirators will communicate using various forms including e-mail to transfer information including debit card numbers.
- b) IMG\_0373 created December 15, 2018 is a photograph of a Verifone POS terminal with merchant ID 9000125884. According to Vantiv/Worldpay records, this merchant ID is associated with Wallace Sleep, Durango, Colorado. This

merchant was a victim of refund fraud for a time period including December 16, 2018.

- c) An e-mail dated December 16, 2018, from ‘Tala Toilolo [proverbs3564life@icloud.com](mailto:proverbs3564life@icloud.com)’ to “John Ward [only1daddy4u@icloud.com](mailto:only1daddy4u@icloud.com)” with message from WARD “Phone broke I don’ know ur number.” The response on December 16, 2018 is 208-9710-3175.
- d) Image IMG\_0378 created December 16, 2018, taken in a room resembling a hotel room with two males identified as Johnathon WARD and Talalima TOILOLO with a POS terminal between them.
- e) IMG\_0401 captured December 18, 2018, with telephone number (208) 970-3175 is an image of a text message between WARD and TOILOLO. WARD states “U try yet need to know if it my thing still”. TOILOLO answers “Let Me check right. I’m”. Based on my experience and discussion with other law enforcement officers, this discussion shows WARD and TOILOLO communicating during the execution of or after a fraud scheme where WARD is attempting to have

TOILOLO determine if a certain aspect of the fraud scheme can still be exploited.

Based upon these photographs and the aforementioned text messages between TOILOLO and WARD, they conducted this fraud scheme and victimized multiple companies over a period of time. TOILOLO and WARD shared information and money and maintained contact during and after the execution of the fraud.

27. On April 25, 2019, Eastern District of California Magistrate Judge Carolyn K. Delaney signed a search warrant associated with Google LLC accounts [still2theleft@gmail.com](mailto:still2theleft@gmail.com), [ognunes100@gmail.com](mailto:ognunes100@gmail.com), and [jwrentals415@gmail.com](mailto:jwrentals415@gmail.com). During the search of the account [still2theleft@gmail.com](mailto:still2theleft@gmail.com), agents found a video captured on July 22, 2018 discussing the above fraud scheme. On the video, WARD makes the following comments:

- “If you oversee all your folks you’re the one that’s going to collect them all then I’m going to deal with one person.”

- “It takes two or three days to pull out that much dough.”
- “I do it one way. I put nine racks on the card, that’s three for me, three for you, and three for this person.”
- “I’ve been doing this for a minute.”
- WARD says people can make “5 cards a week for \$4500”

Based on my experience and discussion with other law enforcement officers, WARD is sharing his knowledge with his co-conspirators about the execution of the fraud and the division of the assets. WARD and his co-conspirators split the proceeds of the fraud. The money is sent to co-conspirators through a variety of methods. During the video, WARD tells these co-conspirators he sends the money online and via money order. WARD specifically mentions that with money orders, co-conspirators do not need to go into a bank.

#### **Wires Associated with TOILOLO**

28. Investigators reviewed of the WARD’s cellular phone seized on October 12, 2018 showed hundreds of messages in various forms including but not limited to text message between WARD and known conspirator Connie RAMOS. On June 9, 2018, an image was sent to WARD from RAMOS’s phone number with a screen shot of a scheduled tax return and the last four number of RAMOS’s social security number. The following is a text stream recovered from WARD’s phone from WARD to RAMOS on June 8, 2018 at 12:49pm to 12:50pm “Send the money to limas mom” “Mahlalela Laloulou” “There waiting on u” “Send the confirmation number to lima”. Based on my experience and discussion with other law enforcement officers, people involved with fraud will attempt to deceive law enforcement about the true nature of the origin of funds use the names of family members to transfer the fruits of the fraud via wire. These methods include but are not limited to sending the money to a trusted family member, instead of the true recipient and listing incorrect information including residence.

29. On July 2, 2018, TOILOLO requests WARD send money to “Catrina Cascarejo”. Catrina Casarejo is the girlfriend of WARD.

30. A text stream from the reviewed WARD cellular phone on October 1, 2018 is as

follows:

- TOILOLO to WARD at 8:35 PM – “Did you get the tracks i sent”
- WARD to TOILOLO at 9:15 PM – “Yeah I got them. It’s going to have to be a three way split because it’s not mine”

“Tracks” are the encoded portion of a credit card on the magnetic strip which contain information about the card including the card number, expiration date, and card owner. The track data showed the cards were registered in the name of Catrina Cascarejo. Based on my experience, people involved in refund fraud would use tracks as the debit cards to execute the refund fraud. In this instance, TOILOLO provided cards or “tracks” which could be used to load the fraudulently obtained refunds. On October 3, 2018, WARD received a text from TOILOLO asking for money. On October 3, 2018, a known co-conspirator wired TOILOLO \$1,000.00 with a pick up location in Salt Lake City, Utah. This money is likely associated with the October 1, 2018 conversation with WARD.

31. On December 17, 2018, RAMOS sent TOILOLO a \$2,500.00 wire transfer. This wire occurred shortly after the refund fraud from Wallace Sleep in Durango, Colorado which TOILOLO and WARD were involved. The \$2,500.00 was likely a payment to TOILOLO from WARD via RAMOS for this fraud.

32. Between 5/7/2019 and 5/19/2019, there were four wires sent for a total of \$3600 from TOILOLO using TOILOLO’s Driver’s license. Using RAMOS’s address in California. These amounts were sent by wire through a system caller Walmart to Walmart to the Walmart Store located at 4627 South 900 East, Salt Lake City, Utah and by money order to a Rite Aid located at 635 E 3300 S, Salt Lake City, Utah. These locations are 2.4 miles and 0.8 miles away from 3355 South Riviera Drive, respectively.

33. On 6/23/2019 and 6/24/2019, Hamilton Wade and Cecilia Wade sent \$3000.00 to Talalima Toilolo in three separate Walmart to Walmart transactions. Hamilton Wade’s criminal history includes but is not limited to a 2011 felony conviction for possession of an assault weapon and 1991 possession of cocaine for sale. Cecilia Wade’s criminal history includes a

2004 felony conviction for committing fraud to obtain aid.

34. Based on my experience, discussion with other law enforcement officers, and my knowledge of this investigation, the wires received by TOILOLO in May and June of 2019 are likely associated with fraud. For the May 2019 wires, co-conspirator RAMOS's address was used. The May and June of 2019 wires fit the pattern of TOILOLO receiving payments after fraud was conducted. In the June 22, 2018 recorded conversation recovered from WARD's phone, he discusses sharing money with co-conspirators and how money orders allow co-conspirators to share money without using a bank.

**Additional Probable Cause that the Locations and Persons to be Searched Contain  
Evidence of a Crime**

35. An open records search showed Catrina Castejillo resided at 3355 South Riviera Drive from February 2018 to July 2019. This was the same address given to WARD by TOILOLO during a text message discussing wiring proceeds of the fraud scheme to TOILOLO on August 1, 2018. A Facebook with user name "Catrina Toilolo" shows a multiple photographs of Catrina Castejillo on her public profile with TOILOLO with the last update in June 26, 2019. A photograph posted March 17, 2019 was "liked" by a known co-conspirator. This residence is identified as a place to be searched in Attachment A-1 below, and TOILOLO is identified as a person to be searched in Attachment A-3 below.

36. The execution of refund fraud requires co-conspirators to maintain equipment used in the execution of the fraud. Additionally, the co-conspirators will maintain lists of victims, credit/debit card numbers, and bank accounts needed to execute the fraud. Co-conspirators keep records including bank records, wire records, and lists of victims. Often, this information is stored at a home residence between times the fraud is executed. It is likely the items used to execute the refund fraud will be found in TOILOLO's residence at 3355 South Riviera Drive.

37. On July 31, 2019, your affiant and other law enforcement conducted surveillance at 3355 South Riviera Drive. Agents observed multiple vehicles at the residence Cadillac

Escalade with Utah license plate number 5F9HU registered to Talalima TOILOLO at 3355 South Rivera Drive, Salt Lake City, Utah. This vehicle is identified as a place to be searched in Attachment A-2 below.

38. The execution of refund fraud requires co-conspirators to travel to banks and offsite locations including hotels to execute this crime. Co-conspirators often store equipment used in the execution of the fraud in their vehicles. From previous search warrants, co-conspirators were shown store equipment in their vehicles. It is likely items necessary to conduct refund fraud will be located in the vehicle registered to TOILOLO.

39. From previous search warrants from WARD's wireless communication devices, communications were observed between TOILOLO and WARD discussing the ongoing fraud scheme including but not limited to victim information and fruits of the fraud. Additionally, WARD's electronic devices contained images and files showing the execution of the fraud scheme. Based on my training, experience, and discussions with law enforcement officers involved in this investigation, it is common for co-conspirators to share and save important information relating to the fraud scheme on their phones for use at a later time. For example, the conspirators in this refund fraud scheme are likely to save digital information relating to POS terminals, victim merchants, TID numbers, credit/debit card information, personally identifiable information of victims of the fraud scheme, receipts of money transfers, co-conspirator contact information, and co-conspirator communications. The conspirators are likely to continue using or consulting this information to continue their fraud scheme. Indeed, the phones seized from WARD's phones in October 2018 contained incriminating records dating back to at least May 3, 2018. Based on my experience and discussions with law enforcement officers involved in this investigation, TOILOLO's electronic devices are likely to contain similar evidence of the refund fraud scheme.

40. There is probable cause to believe that wireless device (e.g., cellphone) account activity will also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the



owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

#### IV. TECHNICAL TERMS

41. Based on my training and experience, I use the following technical terms to convey the following meanings:

a) Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b) Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including

data unrelated to photographs or videos.

- c) Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d) GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.
- e) PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or

miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f) Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, which is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

g) IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static-that is, long-term-IP addresses, while other computers have dynamic-that is, frequently changed-IP addresses.

h) Cloud network: Information and data is stored on physical or virtual servers, which are maintained and controlled by a cloud computing provider. Customers may access stored information on the 'cloud', via an Internet connection.

i) Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

42. Based on my training, experience, and research, I know that the Devices have capabilities that allow them to serve as wireless telephones, digital cameras, portable media players, GPS navigation devices, PDAs, and/or Internet-accessing devices with IP address information. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

**V. ELECTRONIC STORAGE AND FORENSIC ANALYSIS**

43. Your affiant is aware that the SA Laura Giouzelis, the case agent in this matter has spoken with FBI Information Technology Specialist (ITS) and Computer Forensic Examiner (FE) Alan Russell Schmidt, who has been a Forensic Examiner since 2006. FE Schmidt is specially trained in computer search and seizure and is certified by the FBI as a member of the FBI Computer Analysis Response Team (CART). FE Schmidt has been a member of CART since 2005 and has conducted numerous searches and seizures involving computers and computer data. FE Schmidt related information to me and/or confirmed information for me as noted below.

44. Based upon my training and experience, and information related to me by agents and others involved in the forensic examination of computers and digital devices including FE Schmidt, I know that modern cellular phones have many of the same capabilities as computers and have increased storage capacity. Based upon my training and experience, and information related to me by agents and others involved in the forensic examination of computers and digital devices, including FE Schmidt, I know that computers and digital devices are often used to store information, very much the same way paper, ledgers, files and file cabinets are used to store information. I know that it is common today for businesses to utilize computers to conduct their business and to store information related thereto. I also know that it is common for individuals to have personal computers and cellular phones and to use these computers and cellular phones to conduct their personal affairs, their business affairs, and to store information related thereto. .

45. Based on my training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are

typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

46. There is probable cause to believe that things that were once stored on the cellular phones may still be stored there, for at least the following reasons:

- a) Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b) Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c) Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d) Similarly, files that have been viewed via the Internet are sometimes

automatically downloaded into a temporary Internet directory or “cache.”

e)

47. Forensic evidence. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the cellular phones were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

- a) Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.
- b) Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c) A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d) The process of identifying the exact electronically stored information on a storage

medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e) Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.
- f) I know that when an individual uses an electronic device, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

48. Nature of examination. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

#### **COMPARABILITY WITH PRIOR INVESTIGATIONS AND EXPERIENCE**

49. Based on my review of the records and documents in this case, my training and



experience, and my discussions with other law enforcement personnel in this investigation, I do not believe contact between any law enforcement and co-conspirators perpetrating this scheme will necessarily result in them destroying or moving all evidence, fruits, or instrumentalities of the crimes. Based on a review of the digital evidence, the refund fraud scheme has continued after law enforcement contact. I am aware that even after contact with law enforcement, individuals involved in schemes to defraud, and attempts to defraud, federally insured financial institutions will not always cease criminal conduct. To the contrary, such individuals often are emboldened, believing they are no longer targets or suspects. I am aware that often such individuals immediately return to obtaining, and altering fraudulently obtained identification and financial information. In addition, individuals retrieve secreted catalogues, saved and profiled contents of fraudulently obtained financial information and property from areas law enforcement did not search or seize. The individuals will then maintain the items in close proximity, including in their residence. Also, the individuals will—after initial discovery by law enforcement—return to obtaining further identification and financial information (including replacement access devices and PIN numbers for replacement credit/debit cards). Of course, I am also aware based on my training and experience that individuals in schemes such as this one, who have not been confronted by law enforcement, also continue their participation in the criminal conduct.

## **VI. CONCLUSION**

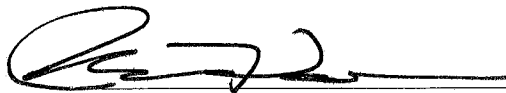
50. TOILOLO utilized his cellular phone to contact co-conspirators and exchange information. Based on my training and experience, people keep their cellular phones on their person, in their vehicle during travel, or in their residence. I submit that this affidavit supports probable cause for a search warrant authorizing the search and examination of the locations and person described in Attachments A-1 through A-3 for the items described Attachment B.

51. Based on my experience and discussion with other law enforcement officers, it is common for people to utilize more than one phone and for phones to store digital information text messages and photographs even if the phone is not actively utilized. Agents will not have


prior knowledge of which phones contain the information which could be used as evidence of a crime and therefore request to seize all phones associated with TOILOLO.

### REQUEST FOR SEALING

52. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the warrant is relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that, online criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness



Justin Hansen  
Agent  
State of Utah Bureau of Investigation  
Federal Bureau of Investigation Task Force Officer

Subscribed and sworn to before me this  day of August, 2019.



THE HONORABLE DUSTIN B. PEAD  
UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A-1**

The residence located at 3355 South Riviera Drive, South Salt Lake City, Utah is described as a one story red brick residence with grey asphalt shingles located on the Eastern side of 3355 South Riviera Drive. A white front door with a white metallic screen door is located on the western side of the house. The numbers "3355" are diagonally affixed to the residence on the right hand side of the front door. A two car detached garage with a white garage door and white aluminum siding is located at the south eastern corner of the residence.

This warrant authorizes the forensic examination of digital and electronic devices at the location for the purpose of identifying the electronically stored information described in Attachment B.

**ATTACHMENT B**

The evidence to be searched for and seized from the locations identified in Attachments A-1, A-2, and A-3, concerns violations of Title 18, United States Code, Sections 1349 (conspiracy to commit bank fraud), 1344 (bank fraud), 1028A (aggravated identity theft), and 1956 (money laundering), whether physical, digital, electronic, or otherwise, involving Talalima Toilolo, Jonathon Ward, Monica Nunes, Connie Ramos for the time period of June 1, 2018 to present, and is described in the enumerated list below:

1. Items, records, and information tending to identify persons exercising dominion and control over the location or particular areas within the location, including correspondence, papers, photos, videos, bank statements, credit card statements, receipts, utility bills, emails, internet transaction records, parcels, mail, and clothing.
2. United States mail, identification documents, and access devices bearing the names of, or otherwise tending to pertain to, persons who do not live at or control the location.
3. Communications between and among Talalima Toilolo, Johnathon Ward, and Monica Nunes or other co-conspirators that pertain to refund fraud, gift cards, theft, or credit and/or debit cards, or that tend to show a conspiracy or participation in a bank fraud scheme.
4. Photographs showing co-conspirators, fruits of the violations, instrumentalities of the violations, indicia needed to execute a credit card or identity theft scheme, including but not limited to photographs of identification cards, purchase receipts, and photographs of credit/debit cards;
5. Documents, records, and information tending to show how money associated with the use of fraudulently obtained point-of-sale terminals or access devices was obtained, secreted, transferred, and/or spent, including purchases of money orders, wire transfers, online purchases, and electronic transfer of funds.
6. Documents, records, and information containing, referencing, or listing the following types of personal identifying information for individuals, businesses or merchants: names, dates of birth, Social Security Numbers, email addresses, telephone numbers, passwords, bank account numbers, credit card numbers, charge card numbers, credit card images, PIN numbers, merchant account numbers, merchant identification numbers (MID), terminal identification numbers (TID), gateway identification numbers (GID), and payment processing account numbers.
7. Point-of-sale terminals and similar devices, including debit/credit card terminals, electronic benefits transfer (EBT) terminals, near field communication (NFC) terminals, electronic funds transfer point-of-sale (EFTPOS) terminals, and magnetic card readers.

8. Credit cards, debit cards, gift cards and documents, records, and information pertaining to the possession, control, ownership, or use of gift cards, including items obtained through transactions involving credit cards, debit cards, and gift cards.
9. Equipment, writings, and software related to the production or editing of counterfeit credit and debit cards.
10. Records and information relating to the access of the email accounts identified in the affidavit, including still2theleft@gmail.com, ognunes100@gmail.com, and jwrentals415@gmail.com, or other online accounts associated with transactions involving point-of-sale terminals, merchant account numbers, gift cards, debit card and/or credit cards.
11. Records and information relating to the internet service provider and Internet Protocol address assigned to the premises.
12. Records and information showing Talalima Toilolo's or any co-conspirator's state of mind concerning his or her execution or participation in any of the violations.
13. With respect to digital and electronic devices, in addition to all of the categories described in the preceding Paragraphs 1 through 12 above, items and information to be seized include any electronic records, including e-mail messages, text messages, videos, electronic documents, images, and/or data:
  - a. tending to identify persons exercising dominion and control over each digital and electronic device searched; and
  - b. tending to place in context, identify the creator or recipient of, or establish the time of creation or receipt of any electronic information responsive to Paragraphs 1 through 12 above.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

The terms "digital devices" and "electronic devices" mean computers, computer tablets (e.g., iPads), electronic storage devices (e.g., hard drives, thumb drives), and mobile phones. The seizure and search of digital devices shall follow the procedures outlined in the supporting affidavit. Deleted data, remnant data, slack space, and temporary and permanent files on the digital devices may be searched for the evidence above.

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “IP address” or “Internet Protocol address” means a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

The term “Internet” means a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.